# AFFIDAVIT FOR SEARCH WARRANT

I, Jacob Green, a Special Agent with the Federal Bureau of Investigation, do hereby state under oath that I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple, Inc., (Apple) to disclose to the government records and other information, including the contents of communications, associated with Apple ID: zayzay0128@icloud.com that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way Infinite Loop, Cupertino, California, 95014. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

1. I am an "investigative or law enforcement officer" of the United States within the meaning of 18 U.S.C. § 2510(7), and empowered by law to conduct investigations and to make arrests for offenses enumerated in 18 U.S.C. § 2516.

2. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since September 2017. Previously, I served as an officer and aviator in the United States Air Force for 12 years and hold the rank of Major. As a Special Agent, I participated in a five-month basic training program at the FBI Academy in Quantico, Virginia. At the FBI Academy, I received training in investigating federal criminal offenses, responding to acts of terrorism, interviewing suspects, performing interrogations, tactical operations and firearms. I have been assigned to the Kansas City Field Office since February 2018. Until June 2019, I was assigned to Squad 12, focusing on International Terrorism. Since June 2019, I have been tasked with investigating criminal enterprises in the greater Kansas City metropolitan area, with a focus on

violent gangs and robbery crews. During my tenure with the FBI, I have been involved in numerous search warrants, informant debriefings, wiretaps, interviews, and arrests. Based on my training and experience as a FBI Special Agent, I have become familiar with the manner in which illegal drug traffickers conduct their drug-related businesses, including the methods employed by drug dealers to import and distribute illegal drugs, and their use of coded language to refer to illegal drugs, drug proceeds, and other aspects of illegal drug trafficking. I have been personally involved in investigations involving the unlawful possession, manufacture, distribution, and smuggling of controlled substances and I have participated in wire intercept investigations.

3. This affidavit contains information necessary to support probable cause for the application. It is not intended to include every fact or matter observed by me or known by law enforcement. The information provided is based on my personal knowledge and observations, information conveyed to me by other law enforcement officials, information discovered through confidential sources, and my review of reports prepared by law enforcement officials.

## ITEMS TO BE SEARCHED AND EVIDENCE TO BE SEIZED

4. This affidavit is in support of a search warrant for the search of records and other information, including the contents of communications, more fully described in Attachment B, associated with Apple ID: **zayzay0128@icloud.com** (hereinafter referred to as "**Target Account**"), described in Attachment A.

5. The records and information sought is stored at premises owned, maintained, controlled, or operated by Apple.

6. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant

to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) from the **Target Account** particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

## OFFENSES UNDER INVESTIGATION

7. Based upon my training and experience and on the facts set forth in this affidavit, there is probable cause to believe the information described in Attachment B associated with the **Target Account** contains evidence of violations of Title 21, United States Code, Sections 841(a)(1) and 846, conspiracy and attempt to possess with intent to distribute and distribution of controlled substances; Title 21, United States Code, Section 843(b), unlawful use of a communication device to commit and facilitate the commission of drug trafficking offenses; Title 21, United States Code, Section 848, continuing criminal enterprise; Title 18, United States Code 1959, violent crimes in aid of racketeering; and Title 18, United States Code, Section 2, aiding and abetting the commission of the aforementioned offenses (hereinafter "**Target Offenses**").

## JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## INVESTIGATION BACKGROUND

8. In June 2017, investigators were provided information regarding a criminal street gang, later identified as "246," operating in the Kansas City metropolitan area. Investigators were advised that Ladele D. Smith (aka "Dellio") had achieved a leadership role in the organization of "246," and was closely supported by David Duncan, Jr. (aka "DJ"), Cory Brown (aka "Twin"), and Martin Garner (aka "Looch"). Since that time, numerous additional members of "246" have been identified, to include Terrance Garner (aka "T-Dot" aka "Dot"), Carleeon Lockett (aka "Tone"), Roy Franklin (aka "Roy"), Sirrico Franklin (aka "Chicco" aka "Rico"), and Gary Toombs. Investigators identified multiple criminal offenses members of "246" and their associates are believed to have participated in, including: homicide, assault, robbery, and illegal drug distribution and trafficking, specifically of Black Tar Heroin (BTH) and marijuana.

9. An investigation targeting the identified members of the "246" criminal organization was initiated by the Kansas City, Missouri Police Department's (KCMOPD) Drug Enforcement Unit and Gang Squad and the FBI's Safe Streets Task Force.

## PROBABLE CAUSE

10. On August 8, 2018, the Honorable Sarah Hays, United States Magistrate Judge for the Western District of Missouri signed a search warrant in case number 18-SW-00288-SWH authorizing the collection of text, data, call detail records, cell site location, and GPS/Precision location of phone number 816-572-0635, a number used by Cory Brown.

11. On August 15, 2018, Brown was observed entering the driver's seat of a black Jeep Grand Cherokee bearing a Missouri Dealer license plate of D5026-AG. KCMOPD attempted to conduct a traffic stop on the Jeep for numerous traffic violations. The Jeep initially stopped. However, when the officer approached the vehicle to make contact with Brown, Brown

fled at a high rate of speed. The officer began pursuing the Jeep, but had to disregard the pursuit based on safety concerns. Brown was driving at a very high rate of speed and in manner that violated numerous traffic laws, and posed a clear and immediate danger to other motorists.

12. The next day, August 16, 2018, investigators received the last GPS location for Brown's phone. Investigators believe Brown discontinued service to the telephone number because of the high-speed chase with law enforcement. Investigators know drug traffickers will frequently change their telephones and telephone numbers to thwart investigative efforts by law enforcement.

13. On August 29, 2018, Carleeon Lockett was arrested while occupying a stolen vehicle. An inventory of the vehicle revealed a bag containing a container of sandwich baggies with a strong odor of marijuana, a black digital scale, a glass jar with apparent marijuana, and a stolen Glock model 33 handgun. Through training and experience, investigators know scales are often used to weigh controlled substances and then the substances are placed into the sandwich baggies for further distribution. Drug traffickers also commonly carry firearms to protect their controlled substances and/or the proceeds from the distribution of controlled substances. Lockett is a known associate of Brown and a member of the 246 organization.

14. On August 30, 2018, a search warrant was issued by the Jackson County, Missouri Circuit Court authorizing the search of Lockett's cellular telephone. A download of Lockett's phone revealed a saved contact for "Twin" with telephone number 816-703-7750. "Twin" is a documented alias for Brown. Lockett's phone also had contact telephone numbers saved for Ladele Smith and David Duncan.

15. On September 12, 2018, Brown was taken into custody on an outstanding arrest warrant from the Circuit Court of Jackson County, Missouri for the felony offense of Resisting a

Lawful Stop related to the incident on August 15, 2018. At the time of his arrest, officers found an iPhone in his pants pocket and three additional iPhones inside his vehicle. Investigators know through training and experience that it is common for drug traffickers to utilize "smart phones" to password protect the contents of the phone and prevent law enforcement from accessing the contents.

16. On September 13, 2018, roughly ten hours after his arrest, Brown was released from custody after he posted a $10,000 cash only bond. A record check of Brown showed he did not have any reported wages from any state in the eighteen months preceding his arrest. Based on training and experience, investigators know that drug traffickers often maintain large quantities of U.S. Currency and generally do not have reported, or legitimate, income.

17. Through training and experience, investigators also know drug traffickers commonly carry multiple phones to communicate with friends/family, customers, and sources of supply for their controlled substances. Investigators also know individuals who deal in illegal controlled substances commonly maintain saved contact lists in mobile telephones, which reflect names, addresses and/or telephone numbers for their associates, to include sources of supply, distributors, and customers, in their criminal organizations. In addition to continuing their illegal businesses, these individuals utilize mobile telephone systems to maintain contact with their criminal associates. In addition, some mobile telephones on the market today have built in electronic digital cameras and video capabilities. Individuals who deal in illegal controlled substances take, or cause to be taken, photographs of themselves, their associates, their properties, their illegal products, and the cash proceeds from these illegal transactions.

18. On September 20, 2018, KCMOPD executed a search warrant at 3708 Bellfontaine Avenue, Kansas City, Missouri. The search warrant was obtained based on prior

sales of crack cocaine at the residence. During the execution of the warrant, Mitchell Byrd was arrested as the sole occupant of the residence. Inside the residence, investigators recovered a handgun, approximately 45.8 grams of crack cocaine, and three cellular telephones. Based on training and experience, investigators know 45.8 grams of crack cocaine is considered a distribution amount of cocaine. One of the recovered telephones had the phone number 816-778-9811. That phone number was the one used by a confidential informant to arrange the purchase of crack cocaine from Byrd on three separate occasions. Byrd is charged in the United States District Court for the Western District of Missouri with possession of cocaine base with the intent to distribute, possession of a firearm in furtherance of a drug trafficking crime, and felon in possession of a firearm.

19. On September 27, 2018, investigators reviewed toll analysis between Brown's phone number 816-572-0635 and Byrd's number 816-778-9811. Between September 2017 and August 16, 2018, there were 649 contacts between the two phones. A review of toll analysis for Brown's phone number 816-703-7750 between August 2018 and September 2018, showed 175 contacts with Byrd's phone, 23 contacts with Lockett's telephone number 816-825-5384, and two contacts with David Duncan's suspected telephone number 816-572-0635.

20. On October 9, 2018, the Honorable Sarah Hays, United States Magistrate Judge for the Western District of Missouri signed a search warrant in case number 18-SW-00366-JTM(SWH) authorizing the search of the four iPhone cellular telephones found at the time of Brown's arrest on September 12, 2018.

21. On October 10, 2018, the four iPhones were transported to the Heart of America Regional Crime Forensics Laboratory (HARCFL) for forensic examination. On October 22, 2018, the four iPhones and the electronic data downloaded from those phones was returned to

investigators. Between October 22 and November 14, 2018, a Special Agent from the FBI examined the data seized from the iPhones.

22. When investigators looked at the iPhone found in Brown's pocket at the time of his arrest, they discovered the passcode was "187187". Investigators know that "187" is a widely used police radio code indicating homicide. Through the forensic examination of the telephone, it was determined the last phone number used by that iPhone was 816-703-7750. The telephone had also used the telephone number 816-969-0912 (hereinafter Telephone 1). The Apple ID associated with the telephone was codexgeo@icloud.com.

23. Between March 29, 2018, and August 24, 2018, there were several conversations between the user of Telephone 1, thought to be Brown because the iPhone was found in his pocket, and the user of telephone number 816-977-8298, saved in the phone under the contact name "Gary." Through the investigation, the telephone number 816-977-8298 has been linked to Gary Toombs, a member of the 246 organization. Telephone 1 contained the conversations documented below.

a. On May 30, 2018, Toombs text Brown stating, "8167298305 Bj. Call that nigga bro. See when he gone hv 2500. He keep lying. I'mma let u deal with it. Lol". Brown responded, "Ok".

b. On June 6, 2018, Toombs text Brown stating, "Call AJ tell him we need our bread. 816 3725027. TODAY! 600". Brown responded, "Ok". Investigators know the term "bread" is a slang term for money. Later that day, Toombs text Brown stating, "I'm in the fortys looking for him now" and "He blocked my phone. I will do THAT NIGGA IN. Let me know".

c. On June 7, 2018, Toombs text Brown stating, "Tell that nigga u want NOW. U bout to pull on Him". Brown responded, "He ain't answer". Toombs insisted, "816

372 5027. Call now." Brown then told Toombs, "I did". Toombs continued by stating, "Again bro. I'm splitting that nigga when I get off. Tell that nigga u what it NOW. FUCK HIM Take no excuse".

24. Through training and experience, investigators know drug traffickers will use specific members of the organization known for violence, or with a violent reputation, to collect debts associated with the illegal distribution of controlled substances. The listed conversations between Brown and Toombs are consistent with Toombs asking Brown to collect debts owed to Toombs and the drug trafficking organization. Investigators also know through the investigation that Brown has a reputation on the street for extreme violence, and has been a suspect in several homicides.

25. On August 29, 2019, the Honorable Matt J. Whitworth, Chief United States Magistrate Judge for the Western District of Missouri signed a search warrant in case number 19-SW-00294-MJW authorizing the collection of information associated with Apple ID: codexgeo@icloud.com. On September 8, 2019, investigators downloaded, unencrypted and examined the iCloud account for Apple ID: codexgeo@icloud.com. As of the date of this application, there has not been anything of evidentiary value found in that data.

26. When investigators looked at one of the iPhones found in Brown's vehicle at the time of his arrest (hereinafter Telephone 2), they discovered the passcode was "0813". Through the forensic examination of Telephone 2, it was determined the last phone number used by that iPhone was 913-306-0386. The telephone had also used the telephone number 816-226-3898. The Apple ID associated with the telephone was **zayzay0128@icloud.com**, the **Target Account**.

27. Between August 25, 2018, and August 27, 2018, there were several conversations between the user of Telephone 2, thought to be Brown because the iPhone was found in his

vehicle at the time of his arrest, and the user of telephone number 404-259-6413, saved in the phone under the contact name “Lazeria Mervin.” Telephone 2 contained the conversations documented below.

a. On August 25, 2018, Lazeria Mervin iMessaged Brown stating, “Lazeria Mervin.” Brown responded, “Ok wat state”. Lazeria Mervin responded, “GA Georgia”. Brown responded, “Its there Walmart”.

b. On August 26, 2018, Lazeria Mervin iMessaged Brown stating, “Hey.. do I need a control number to pick up the money”. Brown responded by sending a photograph of a Walmart receipt for a $150 money transfer. The receipt had reference number 761816836, and showed the sender of the money was Cory Tremaine Brown, 3002 Quail Creek Drive, Independence, MO. The recipient information was cut off, but the following was visible, “AZERIA MERVIN”.

c. On August 27, 2018, Lazeria Mervin iMessaged, “Good Morning, I’m about to add money to your phone, add it to this number?” Brown responded, “Yes.”

28. Through training and experience, investigators know drug traffickers will often use money transfer services like those offered by Walmart to transfer cash and avoid the tracing and documentation of the transaction through a bank. Investigators also know through training and experience that individuals involved in drug trafficking organizations will have other people make payments on their phone bills to assist with the illegal distribution of controlled substances. The listed conversations between Brown and Lazeria Mervin are consistent with Brown asking Lazeria Mervin to make a payment on a telephone bill for a telephone number used by Brown, which is consistent with techniques used by drug traffickers.

29. In December 2018, investigators met with a confidential human source (CS) to discuss 246 and several of its members, including Terrance Garner. The CS said Garner was being supplied with marijuana and regularly carried wads of cash so large they could "not even be folded in half, or rolled up." The CS knew Terrance Garner to sell ounces of marijuana, as well as up to and including "QPs" or quarter pound quantities of marijuana. The CS has been a documented confidential source for the FBI since December 2018. The CS has provided observations and background information regarding 246. The CS is working for monetary compensation, and for consideration regarding potential charges related to being the getaway driver for a homicide suspect. Information the CS has provided to date has been verified by investigators and found to be reliable. The CS has a felony conviction for possession of a controlled substance, and is currently in state custody charged with murder for his alleged role in being the driver during the homicide, and for a separate shooting involving a dispute with a family member.

30. On January 9, 2019, the CS conducted a controlled purchase of approximately 242.2 grams of purported marijuana from Garner. On January 17, 2019, the CS conducted a second controlled purchase of approximately 237 grams of purported marijuana from Garner. After both transactions, investigators were able to smell a strong odor from the green leafy substance provided by Garner. Based on training and experience, investigators know the odor was consistent with marijuana. On February 12, 2019, the CS conducted a controlled purchase of approximately 52.6 grams of purported BTH. Investigators field tested the substance which indicated the presence of heroin.

31. Through the controlled purchases from Garner, investigators were able to determine he used telephone numbers 816-825-6334 and 816-383-9350 to conduct his illegal

drug trafficking. On February 26, 2019, the Honorable Beth Phillips, Chief District Judge for the Western District of Missouri signed an Order in case number 19-WT-00001-RK authorizing the interception of electronic and wire communications from those telephone numbers associated with Garner. On March 27, 2019, the Honorable Roseann Ketchmark, District Judge for the Western District of Missouri signed an Order authorizing the continued interception of electronic wire communications to and from 816-383-9350 and the initial interception of wire and electronic communications to and from 816-678-7748, an additional telephone number used by Garner.

32. While monitoring calls to and from Garner's telephones, investigators began to intercept numerous calls indicating Garner was increasingly paranoid of law enforcement surveillance. On March 11, 2019, investigators intercepted a call to Garner's phone number 816-383-9350 from 816-372-3404. In the call, Garner refers to the user of 816-372-3404 as "Twin," which is the known alias for Brown.

33. During the intercepted call, Garner and Brown discussed instances where both had been followed by unmarked police surveillance vehicles. Brown stated, "I'm just driving, just driving. They everywhere, I'm like shit. I ain't had nothing, I ain't give a fuck." Garner appears to commiserate with Brown by stating, "They keep doing that shit Twin, they gettin on my nerves boy . . . they got, they got a white one, a gray one. They got a blue one, they got three Durangos, yeah they trying to switch they shit, but they still got some of the old ones." Based on training, experience, and the context of the conversation, investigators believe Garner was describing the different surveillance vehicles he had observed following him. Later in their conversation, Garner asked Brown, "But I'm saying so, when you say you be switching up. Do you switch your main number every month too?" Brown replied, "I switch every one of them,

my creep phone, my everything." Based on training, experience, and the context of the conversation, investigators believe Garner was asking Brown for advice on how often to change his telephones and telephone numbers. Brown advised to switch telephone and telephone numbers every month. Investigators know people involved in drug trafficking often utilize multiple cellular telephones and telephone numbers to separate their contacts with family or friends and their contacts with suppliers and drug customers. In this conversation, Brown referred to his "creep" phone, which investigators believe, in the context of this conversation, is a reference to the phone Brown uses for illegal drug trafficking.

34. After Brown said he changed his telephones and telephone numbers every month, Garner replied, "Damn, boy, you do a lot of fucking work boy, so I'm saying but like. So what you do, you just call all your people and just be like woo what." Brown replied, "*Yeah, just call and hit em peeps. That's why I got all iPhone you know, you got the iCloud so when you download your iCloud your other next phone, all your shit pop up. Everything pops up*." Investigators believe Garner is asking Brown how he notifies his drug customers and suppliers of his new telephone number if he switches it so often. Brown then told Garner he uses an iCloud account to save "everything," which investigators believe refers to saved contacts and telephone numbers, call logs, texts, apps, GPS location, and emails. Brown then explained that once he gets a new iPhone, he transfers all of his saved data to the new phone via the iCloud.

35. After Brown explained the process of using the iCloud, Garner asked, "So they can't get at you on your iCloud?" Brown said, "No, so you get iCloud. You know they can't get in that shit. That's like, that's why they hate Apple so much." Investigators believe this portion of the conversation is Brown informing Garner that law enforcement cannot access iCloud accounts, which leads law enforcement to dislike Apple products. Brown and Garner have

further conversation on where to buy and sell iPhones, to minimize the amount of money spent on telephones.

36. On July 29, 2019, another FBI confidential human source (CS-2) conducted a controlled purchase of cocaine from Roy Franklin and Sirrico Franklin. During that transaction, R. Franklin stated, "I swear to God bro, this nigga Twin had a half a brick in the car one day right, he used to just ride around and just bust zip serves all day. Bro, when he had that white 745, nigga we drop Rontez off at his probation class. Bro [unintelligible (U/I)] we in this mother fucker serving in the back seat. Bro, why this nigga take the zip lock bag and go. Nigga that shit went all in the car. That was when we all [U/I]. I said, 'ahhhh,' I jump out. I see Twin jump out. I said, 'this nigga tryin to kill us.' I said 'bro, you tryin to send all of us to jail?' That nigga said, 'my bad, bro.' Then, S. Franklin said, "So he had to take a loss." "Twin" is the known alias of Brown. CS-2 is a documented confidential source for the FBI. CS-2 has provided personal observations and background information regarding 246. CS-2 has also conducted controlled purchases of marijuana and cocaine from 246 members. CS-2 became a documented confidential source in June of 2019 and remains active. CS-2 is working for monetary compensation, and for consideration regarding potential charges for a possession of a controlled substance case in Jackson County, Missouri. Information CS-2 has provided has been found to be reliable. CS-2 has a felony conviction for possession of a controlled substance.

37. On September 9, 2019, a preservation request for the **Target Account** was sent to Apple.

38. Based on the foregoing, investigators believe Brown continues to commit one or more of the **Target Offenses**. Brown has been arrested in the possession of multiple iPhones. During the forensic examination of the iPhone found on his person, investigators found

conversations related to the collection of money or debts owed to Brown and other members of the organization, indicating the phone is used in furtherance of the **Target Offenses**. In an intercepted telephone call, Brown explained to another drug dealer how to avoid investigative efforts by law enforcement by changing cellular telephones and telephone numbers every month. In that conversation, Brown mentions changing his "creep" phone, which investigators believe is a reference to the phone he uses in furtherance of the **Target Offenses**. Brown further stated he only uses iPhones so he can transfer saved information and data between phones utilizing an Apple iCloud account. The iPhone found in Brown's vehicle at the time of his arrest was linked to the **Target Account**. During the forensic examination of the iPhone found in his vehicle (Telephone 2), investigators found conversations related to the transfer of money consistent with drug trafficking, indicating the phone was used in furtherance of the **Target Offenses.** Brown also believes law enforcement cannot access his iCloud account, the **Target Account**, leading investigators to believe there is additional evidence of the commission of the **Target Offenses** in the **Target Account**.

## INFORMATION REGARDING APPLE ID AND iCLOUD

39. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

40. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

41. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

42. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user

accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

43. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

44. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

45. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

46. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated

with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

47. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

48. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on training and experience investigators know, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

49. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device

identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

50. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

51. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

52. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

## CONCLUSION

53. Based on the forgoing, I request that the Court issue the proposed search warrant.

54. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

**REQUEST FOR SEALING**

55. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Jacob Green
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn to before me this 17th day of September 2019.

Honorable Lajuana M. Counts
United States Magistrate Judge
Western District of Missouri